BakerHostetler

Baker&Hostetler LLP
One North Wacker Drive
Suite 4500
Chicago, IL 60606-2841
T 312.416.6200
F 312.416.6201
www.bakerlaw.com
Aleksandra M. S. Vold
direct dial: 312.416.6249
avold@bakerlaw.com

February 5, 2021

VIA OVERNIGHT MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Attorney General MacDonald:

We are writing on behalf of our clients, The Nebraska Medical Center ("Nebraska Medicine") and University of Nebraska Medical Center ("UNMC"), to notify you of a security incident involving one New Hampshire resident.[1] Nebraska Medicine and UNMC are Affiliate Covered Entities under the Health Insurance Portability & Accountability Act ("HIPAA"). The entities also share an IT infrastructure and information security personnel.

On September 20, 2020, Nebraska Medicine/UNMC identified unusual network activity. Nebraska Medicine/UNMC immediately took steps to secure the network and began an investigation with the assistance of a computer forensic firm. The investigation determined that an unauthorized person gained access to the network between August 27, 2020 and September 20, 2020. During that time, the unauthorized person deployed malware and acquired copies of some of the information on Nebraska Medicine/UNMC systems. On September 24, 2020, Nebraska Medicine/UNMC determined that the acquired information included documents that contained patient information. Nebraska Medicine/UNMC immediately began a comprehensive review of all documents involved to determine what information may have been accessible to the unauthorized person. Through this review, Nebraska Medicine/UNMC determined the documents may have included the name, date of birth, Social Security number, and/or clinical information for one New Hampshire resident.[2]

[1] This notice does not waive Nebraska Medicine/UNMC's objection that New Hampshire lacks jurisdiction over either entity regarding any claims related to this incident.

[2] Please note that additional New Hampshire residents are being notified pursuant to HIPAA, but the information identified for these individuals does not constitute Personal Information as defined by N.H. Rev. Stat. § 359-C:19(IV).

On February 5, 2021, Nebraska Medicine/UNMC will mail a notification letter to the New Hampshire resident pursuant to HIPAA (45 CFR §§ 160.103 and 164.400 *et seq.*) and N.H. Rev. Stat. § 359-C:20(c), in substantially the same form as the enclosed letter. Nebraska Medicine/UNMC are offering the individual a complimentary one-year membership to credit monitoring and identity theft protection services. Nebraska Medicine/UNMC have also established a dedicated, toll-free call center where all individuals may obtain more information regarding the incident.

To help prevent something like this from happening again, Nebraska Medicine/UNMC are continuing to regularly audit their systems for potential unauthorized activity and have implemented and will continue to implement enhanced network monitoring tools.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

Aleksandra M. S. Vold
Partner

Enclosure

UNMC
Nebraska Medicine

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

<<b2b_text_1(CompanyStatement)>> seriously the confidentiality of our patient's information. Regrettably, we are writing to inform you of an incident involving some of that information<<b2b_text_2(CompanyStatement2)>>.

On September 20, 2020, we identified unusual network activity. We immediately took steps to secure the network and began an investigation with the assistance of a computer forensic firm. The investigation determined that an unauthorized person gained access to our network between August 27, 2020 and September 20, 2020. During that time, the unauthorized person deployed malware and acquired copies of some of the information on our systems. On September 24, 2020, we determined that the unauthorized person acquired copies of documents that contained patient information. We conducted a review of all documents involved and determined that one or more files contained your information. This may have included your name, address, date of birth, Social Security number,<<b2b_text_6(AdditionalDataElements)>> health insurance information, medical record number, and/or clinical information, which may have included physician notes, laboratory results, imaging, diagnosis information, treatment information, and/or prescription information.<<b2b_text_3(ImpactedDataStatement)>>

We have **no** indication that any of your information has been used to commit fraud. However, in an abundance of caution, we wanted to notify you of this incident to assure you that we take this matter very seriously. As a precaution, we are offering you a complimentary one-year membership of Experian IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection support focused on immediate identification and resolution of identity theft. IdentityWorks℠ Credit 3B is completely free to you, and we understand that enrolling in this program will not hurt your credit score. We also recommend that you review the statements you receive from your healthcare provider and health insurer. If you see any charges for services that you did not receive, please call the provider or insurer immediately. For more information on identity theft prevention and instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.

We deeply regret that this incident occurred and for any concern this may cause you. To help prevent something like this from happening again, we are continuing to regularly audit our system for potential unauthorized activity and have implemented and will continue to implement enhanced network monitoring tools.

If you have any questions, please call 1-855-763-0482, Monday through Friday, between 8:00 a.m. and 5:30 p.m. Central Time.

Sincerely,

Debra Bishop
Privacy Officer
<<b2b_text_4(SignatureText)>>

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: **<<(EnrollmentDeadline)>>** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: **www.experianidworks.com/3bcredit**
3. PROVIDE the **Activation Code: <<Member ID>>**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **1-???-???-????** by **<<(EnrollmentDeadline)>>**. Be prepared to provide engagement number **<<(EngagementNumber)>>** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at **1-???-???-????**. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax,* PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian,* PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion,* PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission,* Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze,** PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze,** PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze,** PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Additional information for residents of the following states:

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office,* 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office,* 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

Rhode Island: Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office,* 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.